**SaaS/Managed Services Security & Readiness Checklist**

**Review Request Form**

Instructions: This form should be filled out by a Montclair State University representative to accompany a completed “SaaS Security & Readiness Checklist” from the proposed “Software as a Service” (SaaS) vendor/provider. It is intended to provide the Information Technology Systems & Security team with necessary background information when evaluating a completed vendor checklist.

Submitter Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Campus extension: x\_\_\_\_\_\_\_\_\_\_

Project/Service Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1) Overview of the services to be provided by SaaS vendor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2) Will the application or services be collecting, storing, or otherwise utilizing PCI-related credit card data? [ ]Yes [ ]No

*If yes*, please describe how credit card data will be used:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3) Is any University data intended to be shared with or stored by the vendor? [ ]Yes [ ]No

*If yes*, please describe the data required:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*If yes*, has the vendor identified the method (upload via secure web interface, secure file transfer, other) for exchanging this data? Please describe:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4) Will Information Technology be responsible for any user or application support related to this solution? [ ]Yes [ ]No

*If yes*, please describe:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Software as a Service (SaaS/Cloud) and

Managed Services (Hosted)

Security & Readiness Checklist

**Overview**

The Software as a Service (Saas) and Managed Services (Hosted) Security & Readiness Checklist applies to situations where Montclair State University is considering an external hosted service such as an application service provider (ASP) or a software-as-a-service (SaaS) provider.

Applications and services hosted by external service providers bring special challenges. Among these are service availability, system and application patch management, network security, data handling and privacy protection, incident response, data backup and disaster recovery procedures.

The ability of Montclair State University to service its students, manage its costs and meet its regulatory requirements may be affected by the products, services and systems that are hosted by third party providers. In selecting a host provider, it is important to take into consideration many factors, such as strategic purpose, business objectives, risks, benefits, legal requirements, costs, needs, financial stability, performance capabilities and technical and operational requirements.

This checklist is a guide for evaluating the security of an external hosting service that will be providing hosting services for Montclair State University information.

|  |
| --- |
| **To be completed by Hosting Provider** |
| Please provide a Yes or No answer to each question. If a question is not applicable, enter “N/A” in the comments section. Please provide details in the comment section when asked or as necessary to complete a question thoroughly. You may attach a separate sheet as necessary. If doing so, please include the question number before each comment. |

**Section 1: General Policies, Procedures and Compliance**

|  |  |  |  |
| --- | --- | --- | --- |
| Question: | Yes | No | Answer/Comments: |
| **1.1** Does your organization have a documented and provable information security policy in place that details your information protection program for both logical (systems and applications) and physical security? (Example list of items included in an information security policy: organization structure, physical security, employee hiring and termination procedures, data classification and loss prevention, access control, server and client systems management & security, network security, remote access procedures, backup and disaster recovery, etc.)  |  |  |  |
| **1.2** Is the information security policy internally reviewed and updated on a periodic basis?  |  |  |  |
| a. What is the frequency of review? (weeks, months) | --- | --- |  |
| **1.3** May a copy of your information security policy be reviewed by Montclair State University’s Information Technology, Purchasing, Auditing, and/or Legal departments?  |  |  |  |
| **1.4** Do you outsource any processing to another third party provider?  |  |  |  |
| a. If Yes, list the names of outsource provider(s).  | --- | --- |  |
| **1.5** If outsourcing is done, have you determined that the security policies of the provider comply with your own?  |  |  |  |
| **1.6** If outsourcing is done, are any of your outsourced providers’ facilities located outside of the United States? If YES, please list the countries in the *Comments* field.  |  |  |  |
| **1.7** In order to protect the confidentiality, integrity and availability of Montclair State University’s confidential information, does your organization ensure that: | --- | --- | --- |
| a. Information and services are provided only to those authorized?  |  |  |  |
| b. Information is protected so that it is not altered maliciously or by accident?  |  |  |  |
| c. Information and services are provided in conjunction with your disaster recovery and business continuity planning policy?  |  |  |  |
| **1.8** Does your organization maintain a business continuity and/or disaster recovery plan? |  |  |  |
| **1.9** Is the business continuity and/or disaster recovery plan internally reviewed and updated on a periodic basis? |  |  |  |
| a. What is the frequency of review? | --- | --- |  |
| **1.10** Does your organization actively maintain an internal document repository accessible to all key personnel for all systems, applications, and data inter-dependencies? |  |  |  |
| **1.11** Does your organization utilize (sub-contract) any hosted services related to the services provided? |  |  |  |
| **1.12** Does your organization maintain PCI-DSS compliance for hosted applications that perform credit card transactions? |  |  |  |
| **1.13** Does your organization maintain HIPAA compliance (specifically the HIPAA Privacy Rule and Security Rule) for hosted applications that store, manipulate or transmit health information? |  |  |  |
| **1.14** Does your organization maintain FERPA compliance for hosted applications that store, manipulate, or transmit student education records? |  |  |  |
| **1.15** Does your organization maintain GLBA (Gramm-Leach-Bliley Act) compliance for hosted applications that store, manipulate or transmit financial information? |  |  |  |
| **1.16** Can a copy of your most recent external audit report be provided to Montclair State University for review? (i.e. SAS70-Type II report, external audit report and/or executive summary of audit)For PCI, please include your most recent PCI audit document. |  |  |  |
| **1.17** Do you have a privacy policy to prohibit the sharing of customer information, except as allowed by privacy legislation exceptions? |  |  |  |

**Section 2: Service Continuity**

|  |  |  |  |
| --- | --- | --- | --- |
| Question: | Yes | No | Answer/Comments: |
| **2.1** Does your organization maintain an active redundant site at another location that can be used in the event of a disaster/failure? |  |  |  |
| a. Approximately how many miles are between the two sites? | --- | --- |  |
| b. Has your organization confirmed the primary and secondary sites are on separate utility grids? |  |  |  |
| c. Does the fail over of services require an interruption to the services provided? If yes, how long would it take to recover the services provided? |  |  |  |
| **2.2** What type of testing do you conduct to maintain the integrity of the redundant sites (i.e. simulation drills, walk-through exercises, tabletop exercises, actual drills, etc.)? | --- | --- |  |

**Section 3: Data Center Facilities & Security**

|  |  |  |  |
| --- | --- | --- | --- |
| Question: | Yes | No | Answer/Comments: |
| **3.1** Does your organization use a co-location facility for any of your sites (primary or secondary)? If yes: |  |  |  |
| a. Does the co-location facility provide a physically segregated container (room, cage, etc.) for your equipment?  |  |  |  |
| b. Is the container locked at all times? |  |  |  |
| c. Is the container restricted to authorized personnel only? |  |  |  |
| d. Does the facility provide monitoring & surveillance? |  |  |  |
| **3.2** Are physical security measures in place to protect Montclair State University data from modification, disclosure, and destruction? |  |  |  |
| **3.3** Are all facilities protected by environmental controls (smoke detectors, fire suppression systems, water sensors, uninterruptible power supplies (UPS), and temperature sensors)? Please detail. |  |  |  |
| **3.4** Is all data center facility access checked for authorization and logged? Please detail procedures. |  |  |  |
| a. Are all visitors required to sign in and be accompanied by an escort at all times? |  |  |  |
| **3.5** Are external audits performed on the physical and information security controls? How often? |  |  |  |
| **3.6** When was the last audit performed? | --- | --- |  |

**Section 4: Data Storage & Protection**

|  |  |  |  |
| --- | --- | --- | --- |
| Question: | Yes | No | Answer/Comments: |
| **4.1** Does your organization maintain active data storage protection (RAID, redundant storage arrays, etc.) If so, list the types in use related to the services provided. |  |  |  |
| **4.2** Does your organization maintain passive data storage protection (file archiving, tape backup, etc.) If so, list the types. |  |  |  |
| a. Does your organization maintain segregated backups for each client or is it co-mingled? |  |  |  |
| **4.3** Are system, application, and data backup & recovery procedures updated and tested periodically? |  |  |  |
| a. What is the frequency of review? Of testing? | --- | --- |  |
| **4.4** What is the estimated time to restore a provided service should you experience a serious business interruption that lasts more than one business day?  | --- | --- |  |
| **4.5** Is access to backup media and data (online and offline) restricted to authorized individuals only? |  |  |  |
| **4.6** Is backup media and data encrypted? |  |  |  |
| **4.7** Is backup media rotated to off-site and secure storage? |  |  |  |
| **4.8** Does your organization utilize it’s own site or a third party provider for off-site backup storage? |  |  |  |
| a. If third party, what is the name of the company? | --- | --- |  |
| b. Do you maintain a log of all storage media by location and content? |  |  |  |

**Section 5: Systems & Network Security**

|  |  |  |  |
| --- | --- | --- | --- |
| Question: | Yes | No | Answer/Comments: |
| **5.1** Does your organization have functionally separate Security and Systems staff and/or departments? Please detail. |  |  |  |
| **5.2** Are your employees/contractors required to sign a confidentiality agreement? |  |  |  |
| **5.3** Do you have a mandatory security awareness program in place for employees to make them aware of confidential information, the company’s security policies and standards and good security practices? |  |  |  |
| **5.4** Are procedures in place for reporting and responding to possible security incidents? |  |  |  |
| **5.5** Is penetration testing conducted at least annually to determine vulnerability of network and to determine the level of damage that could occur if compromised? |  |  |  |
| **5.6** Does your organization use a local Intrusion Prevention System(s) IPS? |  |  |  |
| **5.7** Does your organization use a local Intrusion Detection System(s) IDS?  |  |  |  |
| **5.8** Do you log unauthorized access attempts to the system and/or network? |  |  |  |
| **5.9** Do you preserve event logs in case of a breach or investigation? |  |  |  |
| a. If so, long are logs retained? | --- | --- |  |
| **5.10** Are logs kept in a secure, central location, separate from the system components? |  |  |  |
| **5.11** Are operating system patches and updates applied in a timely manner? |  |  |  |
| **5.12** Is appropriate anti-virus software employed and regularly updated?  |  |  |  |

**Section 6: Application Security**

|  |  |  |  |
| --- | --- | --- | --- |
| Question: | Yes | No | Answer/Comments: |
| **6.1** Are logical security measures in place to protect Montclair State University’s data from modification, disclosure, and destruction?  |  |  |  |
| **6.2** Will Montclair State University application data be securely segregated from the data of other customers? |  |  |  |
| **6.3** Will encryption be used on any of Montclair State University data? If YES, please indicate the encryption to be used and where in the *Comments* field. |  |  |  |
| **6.4** Who within your organization or at a sub-contractor's organization will have access to Montclair State’s data? | --- | --- |  |
| a. Under what circumstances are they authorized to handle/view our data? | --- | --- |  |
| **6.5** Is there a documented process to verify a requester's identity and the need-to-know before access is given to Montclair State University information? |  |  |  |
| **6.6** Are reviews conducted to validate that user access is appropriate? (i.e. inactive accounts, employees who have changed job responsibilities or who have terminated employment) |  |  |  |
| a. If yes, what is the frequency? | --- | --- |  |
| **6.7** Do you immediately disable or modify access entitlements when an employee’s status changes (termination, transfer, etc)?  |  |  |  |
| **6.8** Who will handle the administration of the users in the application(s)? (Montclair State, your organization, others) | --- | --- |  |
| **6.9** Do you log unauthorized access attempts to the application(s)? |  |  |  |
| **6.10** Do you preserve user event logs in case of a breach or investigation? |  |  |  |
| **6.11** Are logs kept in a secure, central location, separate from the system components? |  |  |  |
| **6.12** How long are logs retained? | --- | --- |  |
| **6.13** Do you have a separate application development environment from your production environment?  |  |  |  |
| **6.14** Is there a separate test environment?  |  |  |  |
| **6.15** Are documented change control procedures in place? |  |  |  |
| **6.16** Does your organization enforce a strong password policy? |  |  |  |
| **6.17** Do you apply application security patches on a regular basis? If YES, please indicate the frequency in the *Comments* field. |  |  |  |
| **6.18** Do you have a defined process for testing and applying critical patches outside of your regular patch cycle? |  |  |  |
| **6.19** Before application patches or updates are applied, will Montclair State have an opportunity to perform validation testing? |  |  |  |
| a. If yes, what is the testing time frame? | --- | --- |  |
| **6.20** If a patch or update causes an issue, are there documented rollback procedures in place? |  |  |  |
| **6.21** For application updates that change or enhance existing functionality, will a 'sandbox' or 'early access' environment be available for Montclair State to perform testing and end user training? |  |  |  |
| a. If yes, what is the testing time frame? | --- | --- |  |

----------------------------

**Service Provider Information:**

|  |  |
| --- | --- |
| Completed By: |  |
| Title: |  |
| Date: |  |
| Contact Information: |  |

**Montclair State University:**

|  |  |
| --- | --- |
| Reviewed By: |  |
| Title: |  |
| Date: |  |
| **Approved: \_Yes**  **\_ No**If No, provide summary explanation. |  |

Acknowledgments

Montclair State University would like to thank Cleveland State University’s Information Technology department for generously providing us with permission to adapt their original document to our specific needs.